Exhibit D

Manual Chapter : Overview

Applies To:

Show Versions

Table of Contents | Next Chapter >>

What is Policy Enforcement?

BIG-IP® Policy Enforcement Manager™ (PEM) facilitates mobile service providers control subscriber traffic. The system can analyze application traffic and subscriber behavior, and then enforce traffic policing rules that you define. For example, you could have the system drop all web traffic coming from certain IP addresses. You can perform QoS actions on traffic you want to be treated as high priority using DSCP marking, link QoS, or bandwidth control. You could redirect HTTP traffic destined for a particular IP address, and send it to a specific URL. Or, you could send all video traffic from certain subscribers to servers for optimization.

The BIG-IP system is inserted between the subscribers and the network they are trying to access. The system intercepts the traffic that subscribers are sending. The goal of the Policy Enforcement Manager is to apply an enforcement policy to a subscriber. To determine what kind of policy to apply to the subscriber, PEM™ needs to obtain the subscriber identity.

The system can obtain subscriber identity by looking at RADIUS traffic (if present), or by analyzing subscriber data traffic. RADIUS provides much more information about the subscriber. Although analyzing subscriber traffic is more limited, it does provide the subscriber IP address. The system must have the subscriber IP address in order for PEM to do policy enforcement.

Here is a typical illustration of how policy enforcement works. Traffic from a mobile service provider goes to the BIG-IP system on its way to a network. In order to regulate subscribers, PEM needs to determine the policy to apply. For that reason, PEM collects subscriber identity by intercepting RADIUS traffic when subscriber logs in to the network and examines (snooping) the RADIUS Authentication and Accounting packets for details about the subscriber. PEM communicates with an external policy server, in this case, PCRF, for dynamic subscriber provisioning. Using the RADIUS information (or the IP address if no RADIUS is present) obtained from the subscriber identity, PEM queries the PCRF for the policy configuration and provisions subscribers dynamically.

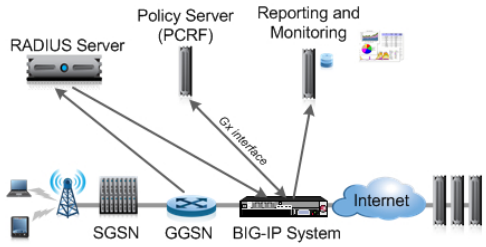

Diagram of policy enforcement overview

Alternatively, you can provision subscribers manually. These subscribers are called ***static subscribers***. You use PEM to add static subscribers one at a time, or to import a list of subscribers. Provisioning static subscribers might require the ability to snoop RADIUS traffic but does not require a PCRF connection, as the policy assigned for static subscriber is pre-configured.

When adding static subscribers on the BIG-IP system, you provide the subscriber ID, subscriber ID type, and one or more policies to apply. You can also specify the IP address, but if it is dynamically assigned, you cannot include it. In this case, you need interception of RADIUS traffic in order to map the subscriber to the IP address. When the subscriber enters the network, the IP address from RADIUS is combined with the information already on PEM. If the static subscriber includes the IP address, no RADIUS interception is required.

About enforcement policies

An ***enforcement policy*** is a set of rules that determines what to do with specified types of traffic. You can configure policies on the BIG-IP® system using Policy Enforcement Manager™ (PEM), or receive policy definition from a PCRF.

For a policy to take effect, it needs to be assigned, or provisioned, to a subscriber session (a subscriber and multiple IP address mapping). A subscriber session is the period of time from when a subscriber logs into the network (authenticated) and logs out, or when the session is terminated by other means. The session is identified by subscriber IP address.

PEM™ supports the following methods for provisioning subscriber policies:

- Subscriber policy provisioning using PCRF
- Subscriber policy provisioning using a subscriber database of static subscribers (up to 100K subscribers)
- Subscriber policy provisioning for unknown subscribers (subscribers that do not currently have policies assigned to them either dynamically or statically)
- Global policy provisioning
- Custom policy provisioning using iRules®

You can use more than one of the subscriber policy provisioning methods. For example, PEM provisions an unknown subscriber policy for a subscriber session, while awaiting a response from PCRF. Or, a global policy might be applied concurrently to other subscriber policies.

As with other BIG-IP modules, like Local Traffic Manager™, you enable PEM functionality by attaching the corresponding profile to one or more virtual servers. To simplify configuration, PEM provides a listener entity that creates the required virtual servers, enables classification, and attaches the policy enforcement profile. When you create a listener, you also define which policies to apply globally or to unknown subscribers.

Advanced users can directly create virtual servers, then configure and attach the Policy Enforcement profile. We recommend that you begin configuring PEM by using listeners instead of using the advanced method. You can get familiar with PEM configuration by examining the virtual servers, settings, and profiles that the listener creates.

About enforcement policy rules

An enforcement policy is made up of a set of rules. In the policy, rules define what to do when the system receives a particular type of traffic. There are many ways you can set up a rule so that you can handle the traffic exactly as you need to. Each rule includes a condition and an action.

A rule defines conditions that the traffic must meet (or not meet) for the rule to apply. The conditions fall into the following criteria:

- ***Classification criteria***, such as applications or categories of applications that the system detects. For example, a rule can apply to all webmail traffic or to a specific webmail application.
- ***Flow information***, such as traffic associated with specific source and destination IP addresses or ports, or incoming DSCP marking. For example, a rule can apply to all traffic directed to a specific destination port.
- ***URL information***, such as URL categories that the system detects. For example, the rule may categorize adult traffic and prevent access to it.
- ***Custom criteria***, which are other conditions that you develop using iRules®

If the traffic meets the criteria in the rule, the rule specifies actions to take, such as:

- Dropping traffic
- Forwarding traffic to a specific endpoint or series of endpoints for value-added services
- Redirecting HTTP traffic to a URL
- Generating reporting data for further processing by external analytic systems
- Usage monitoring about the traffic to the PCRF so it can track mobile usage.
- Setting DSCP bits in the IP header of the traffic by marking all or marking upon the traffic exceeding a threshold
- Setting Layer 2 Quality of Service (QoS) levels for the traffic
- Enforcing rate control using a bandwidth control policy

Because rules provide so much flexibility, you need to plan what you want to do, and consider your options before you add the rules. One option is to simply classify traffic and review reports of the types of traffic your system is receiving to get more information on which to base the rules. This could be the first step when developing enforcement policies using PEM.

About subscriber provisioning through PCRF

When you are provisioning subscriber policies through PCRF, the policies are communicated using Gx interface in the form of Policy and Charging Control (PCC) rules. A PCC rule can contain the complete rule definition, or it might refer to a predefined or dynamic policy rule, as defined by the Gx protocol specification, Release 9.4. See the 3GPP TS 29.212 specification for details. When the complete rule definition is sent, it is a dynamic PCC rule; when the rule is referenced by name, it is called a predefined rule.

A ***predefined PCC rule*** on PCRF maps to an enforcement policy in PEM™. For example, a predefined PCC rule with the name `premium-video` on the PCRF applies to video traffic for premium subscribers. In PEM, you can create a policy also called `premium-video` with policy rules that define the enforcement action. The classification criteria for the traffic is video, and the action could be to enforce QoS for the video traffic (for example, specifying a higher bitrate).

A ***dynamic PCC rule*** is dynamically provisioned by the PCRF over the Gx interface. In this case, the PCC rule contains the rule definition. Therefore, in this case, you do not need to create policies on the BIG-IP® system, since the policy is totally defined on the PCRF.

Best practices for creating enforcement policies

Follow these general recommendations when creating enforcement policies:

- When creating enforcement policies you plan to apply globally or to unknown subscribers, include the word `global` or `unknown` in the policy name to distinguish these from other types of subscriber policies.
- Be cautious when developing enforcement policies to be applied globally. The policies affect all the subscribers and are applied to subscriber policies in parallel.
- When you remove or disable an enforcement policy, first be sure that it is not currently assigned to any subscribers. At least one policy must be assigned to a subscriber at all times.
- Assign the subscriber IP address when creating static subscribers that include a global or unknown subscriber policy, to ensure that the subscriber gets the entitled service faster and does not have to wait for processing of RADIUS traffic.
- If you want to use different types of steering, create separate policies and rules. For example, consider creating a policy that steers traffic from a source VLAN to an endpoint, and another policy to steer VLAN traffic to a service chain.
- Create an empty pool and use it in a forwarding endpoint if you want to route traffic or resolve policy priority conflicts between routing and steering.

These are best practices when writing policy rules:

- Be careful when you mix both L4 and L7 classification criteria in one rule; in some cases, L4 criteria takes precedence. Keep it simple: one rule, one type of criteria.
- Specify different precedence values for the rules that might conflict, to make clear in what order the rules will be evaluated.
- Do not mix different types of policy actions in the same rule; create separate rules for forwarding, reporting, Quality of Service (QoS) actions and finally, for which policy action is implemented.
- A policy (or a rule) should not direct traffic to both a forwarding endpoint and to a service chain. If both are specified, the service chain always takes precedence and is performed first, then traffic is forwarded to the endpoint.
- Dedicate certain bandwidth controllers for use only in PEM™ QoS actions, and do not use them outside PEM.
- One dynamic bandwidth controller can be applied per direction per subscriber and up to eight static bandwidth controllers can be applied, in PEM™.

There are best practices to consider when setting up reporting in enforcement policies:

- Choosing more frequent intervals for generating periodic reporting records (particularly session-based) can greatly increase the amount of reporting data, and could potentially overload the analytics system.
- Flow-based records are generated several times during the flow life and can significantly impact the amount of reporting data sent.

Here are best practices to consider when setting up iRule action:

- If multiple PEM iRules® match a flow, all the iRules are processed. The priority order is as follows:
  - PEM policy priority, and it takes in to consideration if the policy is a global high precedence policy, subscriber policy or low precedence policy.
  - PEM iRule event priority and the default event priority is 500. The event priority can be changed by specifying the priority within the iRule event.
  - Rule precedence.

About sizing considerations

Currently the maximum number of applications or category IDs that PEM™ can store, or report usage statistics for, is limited to 15 per subscriber. This in turn influences the rules, since the traffic statistics for each application or category ID is part of the rule's classification criteria.

When this limitation is exceeded for a given subscriber, an error message is logged into TMM log file. In addition, if the affected rule is installed by PCRF (over Gx connection), a session provisioning failure report is sent back to PCRF. The application or category IDs limitation should be taken into account when designing the subscriber and global policies for a particular PEM deployment.

Note: *If you require granular reporting for large amount of traffic, your performance might be impacted.*

Real performance depends on various factors such as:

- Turning on flow reporting (both performance and memory impacted)
- Frequency of sending session based reporting
- Complexity of classification
- The number of concurrent flows per subscriber
- Over subscription

Table of Contents | Next Chapter >>